

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-22 are currently pending, Claims 1, 9, 11, 19, 21, and 22 having been amended. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, on Figs. 6-8; and page 32, line 24 to page 33, line 9.

In the outstanding Office Action, Claims 1, 3-5, 11, 13-15, and 21 were rejected under 35 U.S.C. §102(b) as being anticipated by Schneier (“Applied Cryptography,” Second Edition); Claims 2, 9, 10, 12, 19, 20, and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Bo Lin et al. (GB 2345229A, hereafter “Lin”); Claims 6 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Kocher et al. (U.S. Pub. No. 2001/0053220A1, hereafter “Kocher”); and Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Kaminaga et al. (U.S. Pub. No. 2002/0124179A1, hereafter “Kaminaga”).

With respect to the rejection of Claim 1 under 35 U.S.C. §102(b), Applicants respectfully submit that the amendment to Claim 1 overcomes this ground of rejection.

Amended Claim 1 recites, *inter alia*,

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups

so that performance of at least one encryption processing unit from one of the groups is performed at a time between performance of encryption processing units from another one of the groups and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed.

In a non-limiting example, Applicants' Fig. 5 shows a conventional authentication procedure between a reader/writer and an IC card. In S101, a random number R_r is input into a triple-DES encryption process, and encrypted data A_1 is generated. In S102, the IC card receives the encrypted data A_1 , and decrypts it to obtain decrypted data A_{1_1} . The decrypted data A_{1_1} is input into another triple-DES process to obtain encrypted data B_1 . Also, the IC card inputs a random number R_c into a triple-DES process to generate encrypted data B_2 . Thus, in the IC card, one group may be the process which inputs A_1 and outputs encrypted data A_{1_1} , while another group is the process which inputs random number R_c and outputs B_2 . Additionally, in this non-limiting example, an "encryption unit" may be a single-DES round within the triple-DES process. Thus, it is clear that there is "each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups," because R_c and A_1 are created completely independently of each other. Applicants' Figs. 6A and 6B show that in a conventional case, these groups would be performed in sequence, such that the process for inputting R_c into a triple-DES process to produce B_2 is not performed until the process of producing A_{1_1} and B_1 is performed. Thus, Fig. 6A is an example of an original encryption processing sequence. However, Applicants' Fig. 8 shows a non-limiting example of the present invention where the sequence is mixed. Fig. 8 shows that the single DESs which are encryption processing units used in the generation of B_2 , are inserted between the single DESs which are used to generate A_{1_1} and B_1 . Thus, these two separate and independent

encryption groups, which have separate and independent inputs (A1 and Rc) are mixed together.

Applicants respectfully submit that the Schneier fails to disclose or suggest the features of amended Claim 1.

Schneier is directed to a description of the Data Encryption Standard (DES) and combining block ciphers. In chapter 12, Schneier describes conventional DES, which includes 16 rounds in which a function which uses a key is applied on a plaintext block 16 times (see pages 270-278 of Schneier). In chapter 15, Schneier then describes ways to combine block algorithms to get new algorithms to increase security without designing a new algorithm. In Chapter 15, Schneier describes Double Encryption and Triple Encryption. In Triple Encryption, a ciphertext block is operated on three times with multiple keys (see pages 357-361 of Schneier). Schneier describes different permutations of Triple Encryption based on the types of keys used (see page 360, describing Triple Encryption with Three Keys and Triple Encryption with Minimum Key). Schneier also describes different modes of Triple Encryption involving Cipher Block Chaining (CBC), such as “Inner-CBC” and “Outer-CBC” (see page 360).

With regard to the feature of “dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units,” the Office Action states that “DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times.” The Office Action also cites to the above-mentioned triple encryption described in Chapter 15 of Schneier. (See Office Action, at pages 3 and page 5). Therefore, it appears that the Office Action believes that a DES block having 16 rounds, the triple encryption in CBC mode, or the triple-DES encryption can correspond to “a plurality of groups composed of one or more encryption processing units.”

However, amended Claim 1 defines that ***“each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups.”*** Therefore, each group in Claim 1 is a separate and independent encryption process with separately and independently generated input data.

However, as presented in the Applicants’ previous response, in the Triple Encryption described by Schneier, including both Inner-CBC and Outer-CBC modes, ***encryption is being applied to a single plaintext file*** (see page 360, for example, where Schneier describes encrypting “the entire file” for each of the Inner-CBC and Outer-CBC modes). Additionally, a single DES with 16 rounds still has just one independently generated input (the initial input), because any subsequent input into any of the later rounds is derived from an input from the previous round. Thus, any one of these processes being described in Schneier constitutes only a single group as defined by Claim 1 because each of the processes described in Schneier is still just directed to a single independently generated input being put through an overall encryption process to produce a single encrypted output.

Additionally, amended Claim 1 defines that ***“said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one encryption processing unit from one of the groups is performed at a time between performance of encryption processing units from another one of the groups and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed.”***

The Office Action takes the position that Schneier discloses “mixing processing sequences of encryption processing units of the plurality of groups with each other,” as recited in previous Claim 1. The Office Action states that this feature is taught by Schneier because “DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times.” The Office Action also refers to the triple encryption techniques described in Chapter 15. (See Office Action, at pages 3 and 5). In other words, the Office Action seems to be interpreting the “mixing” of the groups in Schneier to be disclosed by the existence of multiple processes (such as the 16 rounds of a DES) within one overall group.

However, Applicants emphasize that Schneier does not disclose or suggest mixing of groups, *where each group is separate and independent from each other with a different and independently generated input*. Thus, a single DES, which has 16 rounds, is still its own group, with one single input into the DES process, according to the definition of a group in Claim 1. Also, a triple encryption or triple-DES process described in Chapter 15 of Schneier is still its own single group because even though it is a more complex encryption process than a single DES, it ultimately still just has one independently generated input (i.e., the inputted plaintext file). Therefore, any one of the processes described in Schneier, cannot on its own include the plurality of groups, as defined by Claim 1, being mixed together. Moreover, Schneier does not, for example, describe the encryption units of one DES process or one triple DES process, being mixed with encryption units of a separate and independent DES process or triple DES process which has a separately generated input (see pages 358-360). Additionally, in the CBC mode, one of the DES processes is clearly dependent on another one of the DES processes (see Fig. 15.1, page 361 of Schneier).

Therefore, Applicants respectfully submit that Schneier fails to disclose or suggest all of “a control section configured to set a mixed encryption processing sequence by dividing an

original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, *each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for a group is different and generated independently relative to the input data to be encrypted for the other groups*, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other *by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one encryption processing unit from one of the groups is performed at a time between performance of encryption processing units from another one of the groups* and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed” as defined by amended Claim 1.

Therefore, Applicants submit that amended Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier.

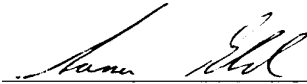
Lin, Kocher, and Kaminaga have been considered but fail to remedy this deficiency of Schneier. Thus, Applicants respectfully submit that amended Claim 1 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Amended independent Claims 9, 11, 19, 21, and 22 recite features similar to those of amended Claim 1. Thus, Applicants respectfully submit that amended Claims 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Sameer Gokhale
Registration No. 62,618